Federal Public Key Infrastructure Management Authority (FPKIMA)

Re-Compete

General Services Administration (GSA)

Federal Acquisition Services (FAS)

Office of Information Technology Category (ITC)

SECTION C
PERFORMANCE WORK STATEMENT (PWS)

C.1 FEDERAL PUBLIC KEY INFRASTRUCTURE (FPKI)

C.1.1 Overview

The Federal Public Key Infrastructure (FPKI) was created out of the E-Government Act of 2002 which directed the General Services Administration (GSA) to establish and operate the Federal Bridge Certification Authority (FBCA). From this initial program, the Federal PKI has grown into a diverse PKI ecosystem of hundreds of certificate authorities (CAs) for federal and state government agencies as well as foreign and US commercial participating PKIs.

The centralized operation and support of the FPKI provides for the tracking, participation, dissemination, and implementation of PKI for the Federal Government to be rapidly and cost-effectively compliant with changes and/or new requirements or orders from several different Federal Government and other policy organizations. These include the Office of Management and Budget (OMB), the FPKI Policy Authority, National Institute of Standards and Technology (NIST), Federal CIO Council, and other similar organizations. Emerging requirements are driven from numerous factors including National Policy, stakeholder needs, technology advancements, or current or future security risks and issues.

The FPKI Trust Infrastructure is the backbone of the FPKI hierarchy. It currently consists of three central certification authorities operated by the FPKI Management Authority (FPKIMA) referred to as FPKI Trust Infrastructure CAs. Any CA in the FPKI can be referred to as a "FPKI CA," but only those operated by the FPKIMA are FPKI Trust Infrastructure CAs. The three main CAs are:

- The Federal Common Policy CA (FCPCA): The trust anchor for the federal Government;
- The Federal Bridge CA (FBCA): The PKI Bridge that enables interoperability between different federal PKIs and between Federal and external PKIs for state, local, or foreign governments as well as commercial entities; and

- The Secure Hash Algorithm 1 (SHA1) and Federal Root CA (SHA1 FRCA): Supports federal legacies that still require the deprecated SHA1 signature hash for certificates.

The FPKIMA has decommissioned the E-Governance CA (EGCA) which supported Identity Credential, and Access Management (ICAM) applications such as metadata signers, relying party application, identity providers, and backend attribute exchanges

C.1.2 Future Objectives and Vision for the FPKIMA

The FPKIMA is committed to building on existing successes with deploying, operating and modifying the FPKI trust Infrastructure CA's to ensure the Federal Government implements and complies with all policy for FPKI functionality, information security, authentication and protection. Internet-related security protocols are evolving rapidly, which requires analysis, extensive collaboration with stakeholders across the federal Government at all levels, and error-free implementation of new functionalities. All activities need to be accomplished with information security engineering, and real-time protection of the infrastructure as a primary focus.

One known, near term, initiative for the FPKIMA is the development and deployment of a new CA to support CA/Browser requirements for Non-Person Entities (NPE) devices as part of Internet of Things (IoT) Federal Government initiatives. A new support contractor is expected to bring the knowledge and capabilities to complete any in-progress development work and system deployments, and to operate the NPE CA in addition to the existing CA's.

C.1.3 Scope

The scope of this acquisition includes:

- Supply of data centers and Internet communications infrastructure meeting DoD Top Secret facility requirements to host GFE-provided systems
- Supply of proactive and disciplined personnel that are knowledgeable and experienced in all relevant technology and operations areas including PKI, networking, virtualization, network management, hardware, security and information assurance
- Supply of a proactive, disciplined and experienced Program Manager that understands and addresses the strategic needs of the FPKIMA and the overall Federal Government, drives organizational effectiveness and change management, and fosters leadership and collaboration across the team
- Operations, Maintenance and Management of FPKI capabilities, network and cloud infrastructures
- Solid design, implementation and operational support for cyber protection
- Design, Implementation, operation, and optimization of virtualized processing environments
- Design, integration, and testing of new technologies for PKI, networking, network management, hardware, security and information assurance

- Analysis and implementation of existing and emerging policies pertinent to FPKI, technical analysis, stakeholder and community support including CA/Browser requirements for NPE devices
- Provides a total personnel solution that includes proactive, comprehensive, and strategy-driven Program Management, Technical Management and Information Assurance Management
- Personnel flexibility at all levels to adapt to the changing Federal PKI and cyber landscape and to address the changing needs of the FPKIMA

C.1.4 Organization of Section C

Section C is organized as follows:

1. C.2 provides an overview of the current FPKI infrastructure that is managed, operated and maintained by the GSA and the existing support contractor.

2. C.3 provides the detailed system requirements for this task order, which encompasses:

    a. C.3.1 – Functional description of the FPKI infrastructure
    b. C.3.2 – General Requirements
    c. C.3.3 – Infrastructure Services
    d. C.3.4 – Technical Services
    e. C.3.5 – Program Management Services
    f. C.3.6 – Ancillary Support
    g. C.3.7 – Information Assurance and Cyber Protection
    h. C.3.8 – Transition-In
    i. C.3.9 – Transition-Out
    j. C.3.10 – Relevant Documentation
    k. C.3.11 – Service Level Agreements (SLA)

C.2 CURRENT FPKI SYSTEM INFRASTRUCTURE

The GSA currently operates, maintains and updates a secure, redundant computing infrastructure to support the FPKI processing capability, comprised of racks, servers, software, firewalls, Intrusion Detection Systems (IDS), etc. The FPKI infrastructure is contained within two Contractor-provided data center hosting facilities along with all internal interfaces, power, HVAC, Internet interfaces and connectivity, etc. to support the GSA-provided infrastructure.

The system is operated as a self-contained, self-hosted cloud service. Rack-based servers provided by the GSA are used to host Virtual Machine (VM) environments that provide the FPKI operational capability.

The system resides outside of all Agency networks. Direct Internet access is provided by the Contractor through GSA-provided (contractor-managed) firewalls and intrusion detection systems.

The Primary Site contains onsite offices as needed for day-to-day operations & maintenance support personnel, and any engineering personnel providing design, testing, deployment, or FPKI operations (e.g. FPKI rekeying). The computing infrastructure is divided into different processing zones to ensure separation of operations and to enforce operational security.

The term "Primary Site" refers to the data center where onsite personnel currently work, where the computing infrastructure production system is located, as well as the lab and pre-production systems. The term "Backup Site" refers to the second data center facility which hosts the redundant infrastructure containing the mirrored production processing capability. The FPKI production infrastructure operates with a "hot-hot" mirrored configuration, so the terms "primary site" and "backup site" designate higher order differences with hosting center equipment and personnel configurations. The lab and pre-production computing capability areas are not mirrored, and are only hosted at the primary site.

- The production system(s) located at the primary and backup sites are housed within a cage at each site that measures approximately 13' by 15'. Only equipment racks and ancillary equipment are installed within these cages.
- The pre-production test system and lab is located at the primary site is housed within cage that measures approximately 13' by 16'. The test system(s) are housed within a single rack; the remaining space is used for tables, chairs, ancillary equipment, storage shelves and a document safe.
- The onsite office at the primary site measures approximately 22' by 50'. There are work areas for 8 staff plus items such as a conference table, misc. work tables for visitors, etc.

C.3 FEDERAL PUBLIC KEY INFRASTRUCTURE (FPKI) SUPPORT REQUIREMENTS

C.3.1 Overview

The Federal PKI is the backbone for identity management throughout the Federal Government. The Federal Public Key Infrastructure Management Authority (FPKIMA) is the technical arm under Federal Identity, Credential, and Access Management (FICAM) and is responsible for the operation of the FPKI Trust Infrastructure. The FPKIMA enables federated and the most cost-effective identity management practices for secure physical, logical access, and information sharing across federal agencies and between external business partners through the execution of digital certificate policies and standards. The FPKIMA ensures the availability of Federal PKI Trust Infrastructure services that are critical to the implementation of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The infrastructure managed by the FPKI provides foundational trust for the U.S. Federal Government's PKI for digital functionality including:

- Personal Identity Verification (PIV) Cards: The FPKI sets policy for and enables technical verification of security certificates installed on PIV cards for all Federal government and contractor employees.
- Computer to Computer Communication: The FPKI sets policy for and enables technical verification of security certificates installed on computers.
- Secure Websites: The FPKI sets policy for and enables technical verification of security certificates installed on web servers.
- Data Encryption and Secure Email: The FPKI sets policy for and enables technical verification of security certificates used to securely encrypt data, both when in transit between two systems, email signing and encryption, as well as when the data is being stored on a system.
- Evolving or future digital functionality to support CA/Browser requirements as part of Federal Government initiatives for Non-Person Entities (NPE) Internet-of-Things (IoT) devices.
- Other/Future initiatives

C.3.2 General Requirements

The FPKI contractor shall supply the required and qualified personnel and the required tools, services, and support to operate, maintain and update all required software, hardware, network equipment (including GFE) and infrastructure to provide the implementation, operation, and maintenance of the FPKI consisting of multiple CAs. These requirements shall be performed in accordance with Federal policies and procedures, including Federal Information Security Management Act (FISMA), Federal Information Processing Standard (FIPS) FIPS-200, FIPS-201, FPKI Certificate Policies, and GSA policies and procedures including the FPKI CP and FPKI CPS.

The contractor shall deliver products, processes, and services, and provide the knowledge, skills and capabilities to fully support the FPKI so it can provide and maintain the full certificate manufacturing processes, publication of certificates and certificate status, revocation of certificates, generation of full-lifecycle management of CA signing keys and certificates, and ensure that all aspects of the CA services, operations, and infrastructure related to certificates as well as those issued under the task order are performed in accordance with the requirements and representations of the task order.

- The contractor shall provide the necessary capabilities to ensure that FPKI products and services are in full conformance with the latest version of X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FPCPF), SHA1 FRCA Policy, as well as FBCA Policy.
- The contractor shall support and deliver FPKI products, processes, services, and capabilities to support the:
    - Generation of encryption/decryption key pairs and key management.
    - Issuance and distribution of cross-certificates.
    - Issuance and distribution of device certificates.

  - Management and dissemination of certificate status information, including Certificate Revocation Lists (CRL)
  - Management and dissemination of certificate status information, including Online Certificate Status Protocol (OCSP) responders, potentially including certificate status "proof sets" (internally signed databases to facilitate OCSP responses) as may be required by the Government. (OCSP is currently used in some related PKI implementations, and the FPKI may be required to support this protocol in the future).
- The contractor shall provide high reliability / high availability processes, equipment, tools and infrastructure to ensure the FPKI infrastructure is operable in support of US Federal Government strategic and operational needs.

The contractor shall deliver FPKI products, processes, services, and capabilities to:

- Support the receipt and transmission of data directly and indirectly with other approved PKI systems and content delivery systems.
- Ensure all FPKI components obtain and maintain synchronized time from a trusted, third-party Network Time Protocol (NTP) service.
- Support the system by providing services that include, but are not limited to, the publication of key management and other certificates including device certificates, as may be required in directories available via the Internet with applicable access controls to prevent modification or deletion of entries.

The contractor shall identify services, capabilities, and technical requirements necessary to support all the required system hardware and software development, integration, and test activities required to provision the FPKI system components in accordance with the RFP and the subsequent issued task order.

The contractor shall ensure that all software utilized or supported on the task order shall be evaluated and compliant with the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408 standard, if applicable.

The FPKI contractor shall maintain compliance throughout the duration of the task order with all applicable Federal, National Institute of Standards and Technology (NIST), and other policies and procedures related to operating Federal IT systems.

All services provided by the contractor shall provide Contingency/Disaster Recovery Planning to support continuity of operations in accordance with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and other related NIST and GSA guidelines, regulations, and standards. Contingency/Disaster Recovery Planning shall provide for the resumption of critical business functions in the predetermined period of time as specified in the FPKI certificate policies and in accordance with the agreed upon Business Impact Analysis and prioritization of resumption of services requirements.

The contractor shall provide strategic and technical consultation and services to the FPKIMA in support of FPKI Certificate Management Services.

All services provided under this Task Order shall comply with the requirements listed in the Alliant contract unless explicitly noted otherwise in this PWS.

C.3.3 Infrastructure Services (*ref. Alliant C.3.1*)

1. The contractor shall provide network Infrastructure support and services. These services include the design and maintenance of the interface/interconnection with all supporting local and wide area network infrastructures, local and global load balancing, and domain name services, including Domain Name System Security Extensions (DNSSEC), IPv6 as appropriate.
2. The contractor shall maintain and operate production systems operating in mirrored configuration at the primary and backup sites. The contractor shall also maintain and operate lab and pre-production capabilities which are compliant with specifications applicable to the production systems.
3. The Contractor shall provide all management and engineering services, personnel, materials, equipment, desktop computing, and office space not otherwise furnished by the Government, necessary to execute tasks in accordance with the contract requirements. The Contractor shall ensure that all staff assigned to the task order can be contacted 24x7 by the GSA by voice, text and email. The GSA may issue devices (e.g. laptops, cell phones) to any personnel supporting the task order at GSA discretion. The FPKI infrastructure shall be configured to send automated system failure messages to personnel that the GSA designates throughout the task order period.
4. Only GFE-owned operations/administration computers shall be used to access GFE infrastructure hosted within the contractor-provided data centers.
5. The contractor shall support the necessary infrastructure, hardware, software, and provide qualified personnel to provide the required secure FPKI services and operations of the production environment 24 hours per day, 7 days per week, including all Federal holidays.
6. The contractor shall support, maintain and improve the necessary mirrored disaster recovery infrastructure, hardware, software, and provide the qualified personnel to provide the required disaster recovery and COOP capabilities such that due to unplanned or planned failure/discontinuity of operations at the production facility, the disaster recovery facility, and test sites can continue to provide service 24 hours per day, 7 days per week, including all Federal holidays.
7. Throughout task order execution, the Contractor shall provide technical advisory services to the Government for the technical refresh, upgrade and refurbishment of GFE.
8. The contractor will maintain the current production (both primary and backup sites), preproduction and laboratory environments within the current facilities for a maximum of six months after task order award.
9. The contractor-provided data center, and communications infrastructure to include Internet connectivity and cross-connect cabling, shall support the necessary GFE hardware and software infrastructure, hardware.

10. The contractor and its subcontractors shall have/utilize a Security Cleared facility that meets DD 254 level compliance for the pre-production test, production and disaster recovery environments, excluding the laboratory systems.
11. The contractor may implement additional sites at future FPKIMA direction.
12. During any infrastructure moves to new sites, or other planned outages for any other purpose, the Contractor shall limit the period of non-redundant system operation to a period not to exceed 24 hours unless FPKIMA approval is obtained by the Contractor. Prior to any planned outage periods, the Contractor shall develop a risk and mitigation plan that addresses issues that can occur with all affected infrastructure items, and develop a mitigation plan. The Risk Mitigation Plan shall encompass physical damage (e.g. broken bolts to dropped equipment), functional damage (e.g. equipment will not power up or operate), and other relevant items. The Contractor shall ensure service contracts are up to date, and arrange for higher support levels with vendors during the move (e.g. drop ship replacement equipment).
13. If directed by the GSA, the Contractor shall provide and temporarily implement duplicate infrastructure to maintain or recover the redundant mirrored operation during any moves or other outage periods. The Contractor shall retain, and turn over to the Government, any hard disks or other data storage devices for any leased equipment that contains controlled unclassified but sensitive data.
14. The contractor shall assist the GSA with implementing energy sustainability goals outlined in multiple legislative acts including the Energy Independence and Security Act of 2007 to pursue a Net Zero energy security posture. The Contractor shall provide for the implementation of "Green IT" concepts and in accordance with the principles of Leadership in Energy and Environmental Design (LEED), and Energy STAR wherever possible in the design, implementation, and utilization of the infrastructure, technical architecture, or facilities according to applicable Government and GSA policies.
15. The Contractor may move the backup site outside of the National Capital Region (NCR) as defined in DoDI 4515.14 to increase geographic distance from the primary site to optimize system survivability. Considerations include:
    a. Located outside of the SERC VACAR power sub-region (http://www.serc1.org/about-serc)
    b. Choice of site locations shall include assessment and minimization of operational impacts to all portions of the overall business model and personnel support.

C.3.4 Technical Services (*ref. Alliant C.3.1*)

The Contractor shall propose, implement, and follow industry-standard and proven processes to provide Technical Services. Contractor personnel shall be proactive, responsive to FPKIMA requests and thoroughly knowledgeable about the technology, standards and policies associated with this infrastructure.

C.3.4.1

C.3.4.2 FPKI-Specific Operational Services

1. The contractor shall provide PKI management services and encryption/decryption key generation/storage.
2. The contractor shall provide full lifecycle Certificate Management services, including generation, modification, re-key, distribution of root and cross-certified affiliate CA certificates.
3. The contractor shall provide Certificate Revocation List (CRL) generation and provide distribution services in accordance with the applicable CPS.
4. The contractor shall provide online, near real-time certificate status via Online Certificate Status Protocol (OCSP) (including hardware/software, licenses and maintenance), with or without proof sets (e.g., software), as may be requested by the Government. (OCSP is currently used in some related PKI implementations, and the FPKI may be required to support this protocol in the future).
5. The contractor shall provide directory management of certificate related items, such as CA certificates, cross-certificates, cross-certificate pairs, CRLs, and authority revocation list (ARL)s.
6. The contractor shall provide system management functions (e.g., security audit, configuration management, continuity of services, and archive.)
7. The contractor shall provide multi-person control of sensitive CA operations, in full conformance with the latest version of FPKI Certificate Policies.
8. The contractor shall provide and ensure multi-factor control, preferably with the use of PIV cards, for all administration. If use of a PIV card cannot be performed, a statement and justification will be required, and the FPKIMA must grant the exception.
9. The contractor shall securely archive and store all FPKI data, including certificates and certificate related data for the period of performance of the task order plus the life of issued certificates, and as required maintain compliance with GSA and FPKIPA specifications. Access to this FPKI data shall be provided to the government and the contractor for the follow-on task order as part of the Transition-Out plan and tasks.
10. The contractor shall ensure all data meets GSA established retention and disaster protection and recovery requirements.
11. The contractor shall support and deliver FPKI support services to:
    a. Track related PKI commercial efforts and advances.
    b. Track PKI issues such as vendor path building issues.
12. The Contractor shall support and deliver FPKI support services to monitor and support the FPKI production environment.
13. The contractor shall support and deliver FPKI support services to coordinate with vendors to distribute the FPKI Common Policy CA root certificate as required as a trust anchor.
14. The contractor shall store and retrieve FPKI content at specified intervals to verify the FPKIA was properly operated in accordance with its policies and practices, including any certificate (including those revoked or expired), issued by the FPKIA. Activities include

daily and weekly log maintenance, controlling and updating architecture information, and annual testing of the FPKIA archive retrieval strategy.

15. The contractor shall provide repository maintenance and monitoring for the centrally managed FPKIA directory system, including maintaining and monitoring the primary and redundant directories, and all interconnections and interfaces to other approved systems.
16. The contractor shall initiate a complete transfer of all current and archived FPKI certificates, validation, revocation/suspension, renewal, policies and practices, billing, and audit data and documents within 24 hours of request, or as otherwise agreed upon, as specified in the task order, and according to Government-approved Data Transfer Plan, as part of the Transition-In and Transition-Out Plans. The data transferred shall not include any data not related to the task order.

C.3.4.3 Infrastructure Operational Services

1. The contractor shall provide operational support and maintenance of the FPKI on-line services 24 hours per day, 7 days per week, including all Federal holidays, during the life of the task order. The services and operations include certificate status verification and validation services, revocation services, disaster recovery, and Continuity of Operations (COOP) services.
    a. The contractor shall provide all other FPKI operations and maintenance services (e.g. laboratory and pre-production test systems), at a minimum, 5-days and a total of 40-hours per work week, Monday through Friday, except Federal holidays, between the hours of 9am and 5pm ET.
    b. The Contractor shall provide and deliver the required on-line services and products for this task order at least in operation and available for use during the required hours of operation, not less than 99.9 percent of the time calculated on a monthly basis (44 minutes/month unplanned outage) and reported in the Monthly Report.
    c. When system hardware or software component failures occur, contractor personnel shall arrive onsite and begin triage within 24 hours of the failure notification when failures of redundant components occur. Otherwise, the Contractor shall be held to the overarching system availability requirements.
    d. All hands-on operational activities (e.g. normal operations, urgent failure response and catastrophic system operation) shall comply with trusted role staffing requirements listed in the FPKI CPS.
2. The contractor shall operate and provide operational and maintenance support for all FPKI supporting software and hardware infrastructure.
    a. This includes support for the FPKI by designing and maintaining all supporting information technology service management functions, including patch management, backup and restore, hardware, firmware, software and application upgrades, internal and external performance and availability monitoring, usage analytics, and virtualization.
    b. The contractor shall provide additional security-related support, including intrusion detection and prevention, security event information management, vulnerability management, certification and accreditation, environmental monitoring and alerting, and physical access control.

3. The contractor shall design, develop, enhance, and maintain tools to support FPKI operations, including tools for certificate analysis, path testing, and other required operations, analysis, management, and testing functions. Analysis capabilities shall include all traffic monitoring and analysis.
4. The Contractor shall operate, maintain, and update tools to monitor all traffic and transactions at any production site, and any additional cloud-based infrastructure (if deployed).

C.3.4.3.1 Fault Monitoring and Management

The contractor shall implement and operate fault management systems and processes to provide real-time surveillance of all solution components. Fault monitoring and management systems shall include an operational dashboard with comprehensive analytics to allow rapid assessment of faults. The network administrator shall be able to specify notification preferences based on pre-set rules. The fault management system shall provide detailed analysis and reports that can prioritize service dispatches for troubleshooting. When fault issues are detected by the system, the fault management system shall automatically send notification to operations personnel.

C.3.4.3.2 Performance Monitoring and Management

The contractor shall implement and operate a performance management system to monitor, at a minimum, all solution hardware and software components. Performance monitoring and management systems shall include an operational dashboard with comprehensive analytics to allow rapid assessment of performance events. The performance management shall be able to provide trend analyses of most congestion or latency problems. The system shall also be capable of reporting the status of specified KPIs and trends. When system performance degrades below some configurable parameter, the performance management system shall automatically send notification to operations personnel.

C.3.4.3.3 Security Monitoring and Management

The contractor shall implement and operate security management systems and processes to provide proactive, real-time surveillance of all solution components. Security events shall be sufficient enough to detect unapproved, abnormal, or anomalous behavior within the infrastructure. All security events shall be logged using configurable rules. Security monitoring and management systems shall include an operational dashboard with comprehensive analytics to allow rapid assessment of security events. The network administrator shall be able to specify notification preferences based on pre-set rules. When security issues are detected by the system, the security management system shall automatically send notification to operations personnel.

C.3.4.3.4 Change and Configuration Management

The contractor shall implement and operate change and configuration management systems to manage all Solution components. The change and configuration management system shall allow for a separate design change request and testing process before the change is deployed, it shall be

able to automate and schedule routine changes, store configuration change history in a database and enforce change policies through workflow templates and standards.

C.3.4.3.5 Patch Implementation and Management

The contractor shall implement and operate a change and configuration management system which supports patch implementation and administration of all Solution components. The Offeror's patch implementation and administration tools shall automatically detect whether specified conditions are met or whether a certain version of the software or patch is installed on the system. The Offeror's patch implementation and administration tools shall be able to acquire the necessary patches, test the patches before deployment, and be capable of automatically deploying patches to a group of components. The patch deployment tool shall also be able to fall back to the previous software version if required. The patch management system shall provide real-time status reports of the software configuration and the patch deployment.

C.3.4.3.6 Version Implementation and Control

The contractor shall implement and operate version implementation and control tools that are capable of storing and controlling the configuration files for the operating systems or system application software used by all Solution components at a minimum. The contractor shall use the version implementation and control tools to guard against accidental alteration of a configuration file and to guarantee a uniform system configuration. The contractor shall also provide a configuration application library to allow network administrators to choose a device version of the configuration file to download to a device.

C.3.4.3.7 Backup and Recovery

The contractor shall implement and operate backup and recovery mechanisms for all solution systems, databases and network devices. The backup and recovery processes for each solution system shall be tested at a frequency that meets GSA IT Policy and validates recovery capability.

C.3.4.4 Design, Procurement, Test and Deployment Services

1. The contractor shall implement the FPKI architecture following GSA PM approval.
    a. The contractor shall develop and/or utilize detailed specifications as needed to support the timely and efficient deployment of the system to production.
    b. The contractor shall apply a rigorous system engineering approach to systematically validate operation (e.g. design review, unit test, integration test, and regression test) in the lab and pre-production areas prior to deployment of new software to the production system.
    c. If the design review or development test process identifies that any additional hardware or software is needed, the contractor shall prepare and deliver a gap equipment list including product, vendor, and estimated cost for approval.
    d. Major milestones include but are not limited to: install, configure, and integrate architectural components; verify and test, refine detailed system design, develop draft and final production installation and configuration instruction; develop draft

and final SOPs; and prepare the system for acceptance testing. The contractor shall conduct the development and test reviews and deliver the documentation and plan specified.

e. The contractor shall report progress of any design and implementation testing campaigns in the Weekly Program Management Report. The report shall identify the tasks, progress, delays with root causes identified, risks, and any recommended solutions.

2. The contractor shall implement the architecture as approved and prepare for and participate in the security A&A process prior to making the system operational.
3. The contractor shall configure the pre-production, primary, disaster recovery, and laboratory site(s) to meet all requirements, assemble, rack and test all hardware; install and configure all software in accordance with the installation and configuration instructions.
4. All work shall only be performed by contractor personnel who have been qualified in trusted roles (see Section C.3.5.6) in the production facilities.
5. The contractor shall integrate reliability, maintainability, and logistic support requirements into the design, development, enhancement, and operations of the FPKI system. Specifically, the contractor shall: design, maintain, and provide services to include high availability (24/7) and fault-tolerant hardware/software redundancy, redundant facilities, failover capability, and automated and manual system monitoring and administration.
6. The contractor shall procure hardware and software necessary for deployment of FPKI infrastructure after obtaining FPKIMA approval. The contractor shall also provide procurement services for hardware and software at FPKIMA request. All licenses must specify the Government as the owner and all purchases approved by the Government. Hardware and software procured for this program, including warranties and software licenses, shall transfer to GFE ownership after installation and integration is completed.
7. The contractor shall integrate and verify the production FPKIA system components to meet the functional, operational, performance, interface, and all other related requirements as stated in this RFP and the subsequent task order. The contractor shall apply, as appropriate, industry and government best practices and standards such as IEEE STD 1012 Standard for Software Verification and Validation.
    a. The contractor shall conduct acceptance testing of the fully integrated architecture, including examination and verification of requirements implemented and, if necessary, refinement of the production installation and configuration instructions and Standard Operating Procedures (SOPs).
    b. The contractor shall document all acceptance test results, any modifications required as a result of failed tests and the subsequent retesting (including regression testing), and make the results available to an independent third-party auditor during the A&A process and with any modification of the system.
    c. Major milestones: test draft installation and configuration instructions, conduct end-to-end acceptance testing of the fully integrated architecture in the lab environment, finalization instructions, finalize SOPs, and prepare acceptance test completion reports.

8. The contractor shall provide fully functional test/lab environments to support the required software, hardware, other equipment, and provide qualified personnel needed to operate and support all required development, testing, production operations, enhancements, change management, and interoperability requirements including, but not limited to:
    a. The laboratory and pre-production test sites shall mirror the FPKIA production environment as much as possible.
    b. Cross-certification testing, including coordination with candidate entity following authorization, conduct technical testing, create and deliver written report on results of testing, identify and resolve potential incompatibilities between the architecture and candidates for interoperability.
    c. Testing proposed changes to the architecture.
    d. Responding to research and development directive relating to issues that affect the FPKIA, and developing recommended solutions for identified operational shortcomings designed to optimize functionality.
9. The contractor shall develop a Master Test Plan describing the overall system Integration and Verification/Test (I&T) plan and schedule, and other key test plans, processes, procedures, tasks, and schedules, and shall provide a detailed, identifiable approach taken for all tests conducted under the Request for Proposal (RFP) and subsequent task order, including the End-to-End System, Integration, and System Acceptance Tests, to obtain Government acceptance of the initial system, upgrades, and changes. This shall include Security Assessment tests as well.
10. For all tests, the contractor shall:
    a. Plan, prepare and conduct all testing activities including Test Readiness Reviews (TRR) and post-test debriefs. Where required, the contractor shall obtain any required permits and Government approvals well in advance of the test due date.
    b. For all major tests, the contractor shall provide to the Government the required TRR package as stated in the task order issued to the contractor.
    c. The contractor shall present the test results to the Government. Following a test, the contractor shall conduct a test debrief and prepare and submit to the Government test reports that include, at a minimum, all test data, test configuration, test logs, results and conclusions.
11. The contractor shall support and provide interoperability testing for future and current FPKI community members. The FPKIMA manages a laboratory system which is used for ensuring new affiliate PKIs CAs and supporting repositories are interoperable with the current FPKIA before receiving their cross-certification, and testing in support of future requirements such as encryption key recovery, new algorithms and technologies (e.g. Elliptic Curve Cryptographic (ECC) algorithm).
12. The contractor shall support and provide the “pre-production” test facilities which mirrors the FPKIA and is used as the “final” test environment prior to implementation of changes to the primary and disaster recovery production sites.
13. In the event the specific roles and responsibilities the FPKIMA change, the contractor shall accommodate change of duties.
    a. [Known/Optional] For FPKI Path Discovery and Validation (PDVal) application testing, the contractor shall maintain a list of certificate path discovery and/or

validation applications that have been tested and recommended for use in the FPKI environment. The contractor shall support and provide capabilities and services to execute tests with the NIST Public Key Interoperability Test Suite (PKITS) for Certification Path Validation and the NIST Path Discovery Test Suite.

C.3.4.5 FPKI Community and Strategic Support Services

1. The contractor shall support various strategic planning, customer briefings, FPKI community support, document development, communications, and support of the Chief Information Officers (CIO) Council and other Government organizations on behalf of the FPKI program support.
2. The contractor shall work with and support FPKI working groups as well as other groups/organizations who are also operating in accordance with the FPKI Program. These groups include, but are not limited to, the FPKIMA team, FBCA TWG, CPWG, PDVal Working Group (WG), FPKIPA, SSPWG, ICAMSC, NSTIC, and CIO-Council. Some of these groups are described further below:

    - Certificate Policy Working Group (CPWG): The Contractor shall assist the FPKIMA with advisory services to the FPKIPA for policy mappings and changes to the FPKI certificate policies
    - Federal PKI Policy Authority (FPKIPA) – the Contractor shall assist the FPKIMA with supporting the FPKIPA to develop and administer PKI policies
    - PKI Shared Service Provider Working Group (SSPWG): The Contractor shall assist the FPKIMA with developing and overseeing processes involved with the PKI Shared Service Provider (SSP) program
    - ICAM Sub-Committee (ICAMSC) – the Contractor shall assist the FPKIMA with supporting the development and update of the ICAM Roadmap and Implementation Guidance, including segment architecture
    - Architecture Working Group – the Contractor shall assist the FPKIMA with developing and updating ICAN technical architectures
    - Citizen Outreach Focus Group – the Contractor shall assist the FPKIMA with developing recommendations concerning solution sets for government to citizen interactions
    - Federation Interoperability Working Group – The Contractor shall assist the FPKIMA with determining business drivers and terms of engagement for inter-organizational trust
    - Logical Access Working Group – The Contractor shall assist the FPKIMA with developing guidance and best practices for Agencies to implement PIV card authentication capabilities

    The Contractor shall provide all necessary support and advisory services needed to support the FPKIMA effort. This includes collaboration with all working groups and FPKI stakeholders. Tasks resulting from these meetings shall be performed in accordance with the tables in Section F.

3. The contractor shall assist the FPKIMA with updating and maintaining a publically available website (currently located at https://www.idmanagement.gov/fpkima/), and its contents, to provide effective information dissemination to the Federal, State, and Local Government stakeholders, companies, and the general public. The Contractor shall also identify areas for improvement to the FPKIMA (e.g. content or site design), and the Contractor shall implement improvements when approved by the FPKIMA.
4. The contractor shall assist the FPKIMA with clear communication to FPKIMA stakeholders by developing a FPKI Knowledge Management repository to support the business and technical requirements and other business rules of the various FPKI stakeholders. This knowledge database shall include internal Standard Operating Procedures (SOP's), technology and policy analysis, presentations, whitepapers, and other technical and strategic analysis requested by the FPKIMA.
5. On occasion, the FPKIMA may require that the Contractor provide Development, Modernization and Enhancement (DME) surge support to accommodate new requirements from the Office of Management and Budget (OMB), the FPKI Policy Authority (FPKIPA), NIST, and other relevant Federal organizations for possible implementation by the FPKI Management Authority. The contractor shall provide all necessary personnel, tools, infrastructure and services. These requirements may be in response to National Policy, Stakeholder needs, technology enhancements or perceived security threats. To be considered DME surge support, the effort shall require an additional 500 hours of work to complete that cannot be accommodated by the ongoing support effort. The Contractor shall provide a proposal, with justifications, as to why these services cannot be accomplished within the core FPKI support services for these DME services. This proposal shall be submitted to the COR and CO for review, negotiation and approval of the scope, tasks, and budgetary items.
6. The contractor shall provide services, processes, personnel, and support should GSA require specific agency technical support, as requested. These support services shall be specifically determined by GSA at a later date during the life of the task order. (This work is non DME)
7. The contractor shall provide services, processes, personnel, and support should GSA require website development and hosting as requested. These services shall be specifically determined by GSA at a later date during the life of the task order. (This work is non DME)
8. The contractor shall provide technical and operational support for transition of the FPKI infrastructure or infrastructure components to/from other providers or the Government as may be required.

C.3.4.6 General Support Services

The contractor shall provide support for trouble ticket tracking and management to the FPKIMA. This support shall include, but is not limited to, the following:

a. The number of trouble ticket reports typically range from 0 to 5 reports per week.

b. The Contractor shall accept and act on problems reported through a multitude of communication paths (e.g. in-person verbally, telephone, or email).
c. The contractor support personnel shall apply industry-standard customer services processes to document the problem, provide assistance to the users, and respond to questions as needed. Problems shall be immediately escalated to operations personnel for further problem investigations.
d. The contractor shall track, manage, execute and close problem report tickets to effectively address and meet stakeholder needs.
e. The Contractor shall report the status of all open problem reports to the FPKIMA in the Weekly Program Management Report. The report shall identify the problem, status/progress, risks, any delays with root causes identified, and any recommended solutions.
f. Contractor personnel shall be available during the normal work week Monday through Friday, except Federal holidays, between the hours of 9am and 5pm EST to address all system problems, or respond to general queries and requests for information
g. The Contractor shall also provide after-hours support to address and correct system outages 24 hours per day, 7 days per week, including Federal Holidays.

The contractor shall provide auditing services. These services shall include, but are not limited to the following:

a. The contractor shall perform, at a minimum weekly, a physical review of the FPKIA, its records (i.e., paper and electronic), and facility to identify any anomalies and to verify operation and maintenance practices are being performed in accordance with all requirements.
b. The contractor shall ensure that a daily physical examination of the facilities is conducted to verify that the environment (e.g., lights and temperature) is properly working and the established safeguards are intact.
c. As part of transition-in and at the request of the FPKIMA, the Contractor shall audit any or all documents, websites, website contents, etc. The Contractor shall identify where items do not yet document the current system configurations and review discrepancies with the FPKIMA. As approved by the FPKIMA, the Contractor shall update documentation to accurately reflect current system functionality, usage instructions, etc. (e.g. remove reference to decommissioned CA's, document functionality not yet captured in the documents).

The contractor shall provide an inventory tracking system and processes.

The Contractor shall support status meetings, reviews, and conferences with the Government to discuss program progress, system availability, issues, enhancements, identify potential problems and resolve identified problems. The Contractor shall generate and deliver Meeting Agendas, Meeting Minutes, Presentation Materials, and an Action Item List for each meeting, review, and/or conference. Copies of all presentation materials must be provided to all GSA representatives at all meetings.

C.3.5 Program Management Services (*ref. Alliant C.3.3*)

The contractor shall propose, implement, and follow industry-standard and proven processes to provide program management services. Contractor personnel shall be proactive, responsive to FPKIMA requests and knowledgeable about the technology, standards and policies associated with this infrastructure.

The contractor Program Manager (PM) shall provide comprehensive strategic direction, effective FPKI program leadership, and knowledgeable technical oversight and support to the FPKIMA. The contractor shall provide an effective and strategic PM who shall anticipate, plan, organize, direct, and control all task order activities for the contractor. The PM shall also notify the FPKIMA about circumstances where the contractor is not adequately prepared to fully or successfully execute some task, and provide a plan to remedy the issue in advance.

The PM, supported by all contractor team personnel, shall ensure that contractor team activities are managed to align with FPKIMA directives, and ensure that activities and work products are compliant with all relevant and evolving federal government policies, directives and instructions. The contractor shall manage and track the functional and technical performance of this task order and that of all subcontracts against the project requirements, deliverables and schedule. The contractor shall develop and provide to GSA reports on this work

The contractor shall provide effective management to ensure effective technical operation; support and improvements are performed for this strategic Federal infrastructure. In doing so, the contractor shall also identify opportunities for efficiencies, including but not limited to innovative approaches, risk reduction, cost and schedule savings, and process improvements.

The contractor shall ensure that all documentation is prepared and distributed to meeting participants in a timely fashion in accordance with Table F-1.

C.3.5.1 Controls and Oversight (*ref. Alliant C.3.3.1*)

The PM shall act as the single official point of contact for the GSA Program Manager (PM), COR and FPKIMA although the government will communicate with any and all Contractor staff on an as-needed basis.

The contractor shall establish and maintain schedules necessary to plan and track contract activities.

The contractor shall submit reports, conduct reviews, and participate in meetings to keep the Government informed of activities, status, risks and mitigations, and miscellaneous topics. The contractor shall modify report contents as directed by the FPKIMA to ensure that data and any graphical analytics meet FPKIMA needs.

The contractor shall provide all necessary services to ensure the contract terms and conditions are met, and that any necessary contract management support activities are provided. The contractor shall support and initiate meetings with the GSA that are needed in order to deliver the

FPKI infrastructure support service. The contractor shall make all personnel available for meetings and briefings in support of the FPKIMA as needed by the FPKIMA or the contractor.

C.3.5.1.1 Program Kick-Off Meeting

Within five (5) days of contract award, the Contractor shall conduct a project kickoff meeting with the GSA, at the 1800 F Street, NW, Washington DC GSA facility. The Contractor shall develop and discuss an agenda based on the contractor's past experience, lessons-learned, and program management best practices. The kickoff meeting shall include the following agenda items:

- Establishing a collaborative team environment and clear communication paths
- Discussion of contract and technical transition-in activities, including issues, risks and mitigations
- Establishing clear understanding of the FPKIMA near-term and longer-term system and technical objectives, challenges, relevant stakeholders, and specific expectations for Contractor engineering and operational support
- Establishing clear understanding of FPKIMA expectations for strategic and leadership support from the Contractor's Program Manager

All contractor key personnel shall attend the kick-off meeting in person.

C.3.5.1.2 Weekly Program Review Meetings

The contractor shall provide comprehensive weekly reporting and analysis of:

- Ongoing work (to include work assigned during ad-hoc meetings, audits, etc.)
- New work planning
- Deliverable progress
- Strategic analysis.
- Schedule and risk issues, mitigations
- Trouble ticket status and root cause analysis
- Contractor program level status and personnel impacts and issues
- Topics shall include transition activities (until complete),
- Work in progress,
- FPKI network health,
- Network utilization and optimization,
- System audits, network reports,
- Information assurance and security,
- FPKI engineering, integration, test and deployment status
- Root cause analysis with detailed description of cause to include hardware, software, infrastructure, documentation, processes and personnel

The contractor shall propose resolutions, with rationale, for all issues for FPKIMA consideration. Activities and resolutions will be implemented as directed by the FPKIMA, and the contractor shall report progress in subsequent weekly review meetings. The contractor shall adjust the

report topics, content, and analytics as directed by the FPKIMA throughout execution of this task order.

C.3.5.1.3 Monthly Status Report

The contractor shall submit a report to the COR each month to comprehensively summarize program status, schedule, and milestone completions. The report shall include:

- Program status, to include objectives met, work completed and work outstanding
- Notable achievements
- Issues or obstacles impeding progress and recommended solutions
- Status of deliverables/milestones
- Issues and resolutions
- Resource planning/status
- FPKI system operational statistics
- Topics or issues identified by the government COR
- Activities planned for the next month

The contractor shall propose resolutions, with rationale, for all issues for FPKIMA consideration. Activities and resolutions will be implemented as directed by the FPKIMA, and the Contractor shall report progress in subsequent reports. The contractor shall adjust the report topics, content, and analytics as directed by the FPKIMA throughout execution of this task order.

C.3.5.1.4 Strategic Analysis and Support

The contractor shall provide as-needed strategic analysis and support to the FPKIMA to address program-related policies, technologies, budgets and miscellaneous requests to address the needs of the GSA and other federal agencies.

C.3.5.2 Risk Management and Mitigation (*ref. Alliant C.3.3.2*)

The contractor shall develop, implement, and execute a comprehensive Risk Management Plan. This plan shall provide detailed processes that the contractor will follow to proactively identify risks, perform risk qualification and prioritization, perform risk monitoring, mitigation and avoidance.

The Risk Management Plan shall be delivered and managed as a part of the overall PMP.

C.3.5.3 Quality Management (*ref. Alliant C.3.3.3*)

The contractor shall develop, implement, and execute a Quality Management Plan (QMP) that addresses Contractor activities and deliverables, and describes how quality of all work performed and all deliverables shall be ensured. The QMP shall provide detailed processes that the contractor will follow to ensure that all work, deliverables including documentation, software, fielded hardware meet GSA, U.S. Government, and industry quality standards.

Contractor processes shall also ensure that deliverables are reviewed for technical correctness, spelling, and clear writing prior to delivery to the Government.

The QMP shall document the processes and measurement methods to measure performance and perform corrective action. The Quality Management Plan shall employ International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 9001:2015, ISO/IEC 90003 and ISO/IEC 9126 standards as applicable.

The QMP shall be delivered and managed as part of the overall Program Management Plan (PMP).

C.3.5.4 Planning and Resource Allocation (*ref. Alliant C.3.3.4*)

C.3.5.4.1 Program Management Plan (PMP)

The contractor shall develop and regularly maintain a Project Management Plan (PMP) describing, at a minimum, the contractor activities, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements for this effort. The PMP shall detail the key activities and milestones, FPKI certificate development status, allocation of staff and other resources necessary for the successful completion of this effort. The PMP shall also address communication and coordination with the GSA, all other relevant Government stakeholders, as well as contractor staff to include subcontractors. The PMP shall address all key management processes associated with this program to include substitution and retention of key personnel, overall personnel staffing, training, cost management, security management, and change management processes.

Whenever the PMP is developed and updated, the contractor shall submit the PMP to the COR in both hard copy and electronic form, Microsoft Word. The initial PMP shall be submitted to the GSA and the contractor shall obtain GSA approval within 90 days of task order award. Based on the PMP, the COR will provide approval to move forward on activities planned. The contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given.

The contractor shall manage the program in compliance with the approved PMP. The contractor shall review and update the PMP quarterly with the GSA and the Contractor shall obtain GSA approval of all PMP updates.

C.3.5.4.2 Financial Management and Reporting

The contractor shall accurately track the task order budget and other financial information. The contractor shall, on a monthly basis, provide accurate and up to date budget information and variances to the GSA COR and GSA PM. The financial report shall be submitted electronically each month to the COR. This report shall provide budget and financial information for each area of the Contractor's WBS structure that is detailed in the Project Plan and agreed to by GSA and the Contractor.

C.3.5.4.3 Staffing Plan and Management

The contractor shall develop, implement, and execute a comprehensive Staffing Plan that documents the staff assigned to the FPKI program, and maps the tasks each is assigned.

Overall, the Contractor's staff shall perform all tasks necessary to operate, maintain and improve the FPKI infrastructure and capabilities. The Contractor shall provide and maintain a qualified workforce as demonstrated by training and skills certification, engineering and operations workforce experience, educational attainments, and security clearances. The Contractor-provided workforce shall be capable of performing all strategic planning and FPKI stakeholder engagement, ongoing operational and maintenance support, technical development, testing and deployment of new assets, including FPKI-specific components.

The Contractor shall provide a minimum of six (6) key personnel, which are:

- Program Manager (PM)
- Information Assurance Team Lead (IATL)
- Information System Security Officer (ISSO)
- Information Assurance Operations Engineer (IAOE)
- Technical Lead Engineer (TLE)
- FPKI Community Team Lead (FCTL)

The overall summary of key personnel duties are described in Section C.3.5.5, however, all key personnel shall be flexible throughout the contract performance period and adjust their specific duties as needed or as directed by the GSA.

Key personnel qualification requirements are listed in Section L. All key personnel shall be in place no later than the first day of the contract period of performance to preclude delays in ongoing projects. Key personnel, as well as non-key personnel, may be assigned to the program on a full-time or part-time basis at Contractor discretion or as directed by the GSA.

The Staffing Plan shall be updated to document change of personnel and task assignments. The Contractor shall provide resumes for all key personnel to the GSA for review and approval prior to onboarding new staff. GSA approval shall be required for all personnel changes, including shift of duties, and adding personnel.

The Contractor's staffing plan shall describe the Contractor's approach and CONOPS for providing ongoing system operational support at the backup site if a catastrophic event occurs in the DC area which causes complete loss of the primary site.

The Program Management Plan, which includes the Management/Staffing Plan, should address all key management processes associated with retention and substitution of key personnel, overall personnel staffing, and training. The Vendor Proposal shall also provide details on processes and other measures they will take to retain key personnel for the duration of this contract. The Vendor shall provide letters of commitment from key personnel.

C.3.5.4.4 Staff Training

The Contractor shall ensure that its personnel assigned to this task order receive necessary training and updates in order to effectively and efficiently perform their duties to meet their specific job roles and overall system operational needs. In particular, those technical staff who provide FPKI engineering support shall obtain necessary training to maintain proficiency on current and emerging technologies for FPKI.

The contractor shall provide initial and annual security and security awareness training for all its prime and subcontractor personnel assigned to this task order to maintain FISMA ATO. The Contractor shall also develop, maintain and provide initial and annual role-based technical training for all personnel assigned to this task order.

The Contractor shall ensure that staff designated as key personnel receive and update training pertinent to their job roles and duties such as:

- Key personnel and/or designated Subject Matter Experts (with FPKIMA approval) shall attend and participate in Government and industry conferences which are relevant to this FPKI support effort. Conferences shall include, but are not limited to, the RSA Conference, NIST security-focused conferences, and other miscellaneous conferences.
- The Contractor shall obtain FPKIMA approval for travel and conference attendance. At least 60 days prior to any conference, the Contractor shall submit pertinent information about the conference to the GSA PM, GSA CO and GSA COR to include:
  - Conference name, location, and description of topics
  - Rationale for attending, including contractor goals that will be met, specific applicability to this FPKI support task, and benefits to the FPKIMA for attendance.
  - Proposed Contractor personnel to be sent, with rationale about the selection of the specific individuals
  - Not to exceed cost
- Conference attendance shall not be authorized without prior approval by the GSA CO, GSA COR and GSA PM.
- For planning purposes, the Contractor should anticipate the need to attend 4 conferences per year as listed below. Please note that the number of conferences and attendees could change.

Location	# FTE	# Days
San Francisco, CA	1	5
Orlando, FL	1	3
Washington, DC	1	4
Chicago, IL	1	5

C.3.5.5 Key Personnel Task Overview

The Contractor shall provide key personnel to support the FPKI solution. Key personnel are considered critical to work performance, providing program leadership, strategic oversight, analysis and vision, and shall remain with the program for at least one year after assignment to the FPKI program to maintain continuity. High level descriptions of the minimum requirements for key personnel are listed below. The Contractor shall adjust specific role tasking to meet system needs throughout the task order period. Key Personnel qualifications are listed in Section H and Section L.

C.3.5.5.1 Program Manager (PM)

The contractor shall designate one person to act as the Program Manager (PM). The PM shall plan, organize, direct, and control all task order activities for the contractor, and its subcontractors; this includes any activities necessary to meet all task order requirements. The contractor PM will act as the single point of contact for the GSA Program Manager (PM), COR, and the FPKIMA. The PM shall provide strategic support and leadership to the FPKIMA and ensure that Contractor team activities are directly aligned with the FPKIMA and overarching Federal guidelines. As part of the Program Management service delivery, the Contractor PM shall provide proven positive and effective leadership that inspires the team including:

- Strategic Thinking: The PM shall formulate objectives and priorities to support the FPKIMA, and implement plans consistent with the long-term interest of the FPKIMA, the GSA and the Federal Government
- Team Building: The PM shall inspire and foster team commitment, spirit, pride and trust
- Conflict Management: The PM shall anticipate and rapidly respond to conflict issues and take steps to prevent non-productive confrontations. The PM shall be tolerant of different opinions but manage them in a positive manner
- Interpersonal skills: The PM shall treat others with respect, courtesy and sensitivity and shall instill those expectations in all team members.
- Oral Communication: The PM shall develop and deliver clear oral presentations, and listen effectively. The PM shall foster these skills throughout the entire Contractor team.
- Written Communication: The PM shall write in a clear, concise, organized and convincing manner for the intended audience. The PM shall foster these skills throughout the entire Contractor team.

The Contractor shall provide the PM with sufficient resources, authority and autonomy to ensure efficient, timely, and effective Program Management support of the contractor team for the FPKIMA. The PM shall ensure comprehensive and accurate delivery of all services and deliverables to the FPKIMA. The PM shall instill and enforce a positive and collaborative unified team approach for the contractor and any subcontractor staff.

The contractor's PM shall present, on a schedule established by GSA, the task order status, progress, risks and issues, budget, change management, quality management, training, and other key task order management metrics to the GSA.

The PM shall periodically assess tools that are utilized to manage the program, and make recommendations for improving efficiencies, and incorporate GSA requests to utilize different tools (e.g. utilize GSA-provided systems such as ServiceNow, Sharepoint, and Google Drive).

C.3.5.5.2 Information Assurance Team Lead (IATL)

1. The contractor shall designate one person to lead the Information Assurance (IA) team. This person shall support the FPKIMA and PM in security matters and their internal chain of command shall be separate from the operations team.
2. The IATL shall ensure that IA team activities are internally coordinated, and externally coordinated with the other Contractor team members and the Government.
3. The IATL shall collaborate with the FPKI Community Team lead, the FPKI Community and the Government on all technical and policy matters related to Information Assurance.

C.3.5.5.3 Information System Security Officer (ISSO)

1. The contractor shall designate one person to act as the ISSO and Information Security Management Advisor and Trainer (ISMA/T). This person shall support the FPKIMA and PM in security matters and their internal chain of command shall be separate from the operations team.
    a. The ISSO-ISMA/T shall comply with GSA CIO P2100.1.
    b. The ISSO-ISMA/T shall have an active DoD Approved 8570 Level 3 certification. .
    c. The ISSO-ISMA/T shall provide security training to all personnel before they can perform activities on this task order. Security training shall include but shall not be limited to requirements from NIST and GSA. The ISSO-ISMA/T shall also undergo all applicable Federal security training.
2. The contractor team, led by the ISSO, shall comply with the required security A&A process and procedures. The contractor shall implement and maintain IT security in accordance with the A&A requirements defined in the FISMA and the e-Government Act of 2002.
3. The contractor shall comply with Federal and GSA continuous monitoring requirements.
4. The contractor shall comply with the required FPKIPA annual and other periodic CP-Certification Practices Statement (CPS) compliance process and procedures. The contractor shall maintain compliance CP-CPS compliance as specified in the applicable FPKI CPs.
5. The contractor shall respond to and resolve security incidents under the leadership of the ISSO-ISMSA/T in accordance with the FPKIMA's procedures. The contractor shall also track and report all security incidents.

C.3.5.5.4 Information Assurance Operations Engineer (IAOE)

1. The contractor shall designate one person to act as the Information Assurance Operations Engineer. This person shall support the FPKIMA and PM in security matters concerning certificate design, implementation and secure operation of the FPKI infrastructure. Their internal chain of command shall be separate from the operations team.
2. The IAOE shall have an active DoD Approved 8570 Level 3 certification.
3. The IAOE shall perform certificate design, integration, testing and operations in a secure manner, and in compliance with all applicable Government and FPKIMA processes and specifications. The IAOE shall coordinate with customer on issuing certificates.
4. The IAOE shall keep appraised about evolving Federal cyber security and PKI policies and initiatives, and inform the FPKIMA about any impacts to the Solution. The IAOE shall maintain a thorough understanding of the CA environment.

C.3.5.5.5 Technical Lead Engineer (TLE)

1. The contractor shall designate one person to act as the Technical Lead Engineer (TLE). This person shall support the FPKIMA and PM throughout the Solution lifecycle. The TLE shall be responsible for the architectural design, performance, and integration for the systems.
2. The TLE shall serve as the contractor's technical point-of-contact for the program. The TLE shall oversee and validate all design, integration and testing of the systems prior to installation into production, ensure that the systems meet all of the Agency's technical requirements, and proactively monitor the overall functionality and performance of the systems with processing FPKI.
3. The contractor team, led by the TLE, shall institute security-focused systems engineering processes into all lifecycle activities to ensure security is a foundational factor that incorporates evolving industry and Government best practices, such as the processes described in NIST 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
4. The TLE shall perform, and ensure the entire team provides, comprehensive analysis and engineering services. Functional design analysis performed by the Contractor that results in recommendations for equipment or software changes shall include cost-performance tradeoffs to assist the FPKIMA with cost-effectively managing the infrastructure and the contractor team.
5. The TLE shall provide the necessary oversight to the operations team to maintain highly available and functional infrastructure and error-free documentation.
6. The TLE shall serve as the transition-in and transition-out manager to ensure a smooth, comprehensive, and collaborative transition process occurs between all parties.

C.3.5.5.6 FPKI Community Team Lead (FCTL)

1. The contractor shall designate one person to act as the FPKI Community Team Lead (FCTL). This person shall support the FPKIMA and PM throughout the Solution lifecycle.

2. The FCTL shall have in depth knowledge about current and emerging FPKI policy and technologies. The FCTL shall assist the FPKIMA with analysis, communications, compliance support, and coordination with all relevant FPKI stakeholders, regardless of Agency.

C.3.5.6 FPKI / Operations Trusted Personnel Task Overview

The Contractor shall provide trusted operations personnel to support the FPKI solution. Trusted personnel are considered essential to work performance, ensuring the day-to-day operations are performed in compliance with FPKIMA policies, and shall remain with the program for at least one year after assignment to the FPKI program to maintain continuity (unless requested by the government for cause).

The Contractor shall provide FPKI and infrastructure operations with multiple staff providing operational oversight as defined in the X.509 CP/CPS documents.

A high level description of the minimum requirements for trusted operations personnel are listed below. The Contractor shall adjust specific role tasking to meet emerging system needs throughout the task order period.

C.3.5.6.1 Officer

The contractor shall provide personnel to perform the role of Officer. The Officer shall provide day-to-day operations of the FPKI, including but not limited to:

- Registering new subscribers and requesting the issuance of certificates.
- Verifying the identity of subscribers and accuracy of information included in certificates.
- Approving and executing the issuance of certificates.
- Requesting, approving and executing the revocation of certificates.

C.3.5.6.2 Operator

The contractor shall provide an Operator, who will be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

C.3.5.6.3 Administrator

The contractor shall provide an Administrator, who shall provide day-to-day operations of the system, including but not limited to:

- Installation, configuration, and maintenance of the CA and Certificate Status Server (CSS) (where applicable);
- Establishing and maintaining CA and CSS system accounts;
- Configuring certificate profiles or templates;
- Configuring CA, RA, and CSS audit parameters;
- Configuring CSS response profiles; and
- Generating and backing up CA and CSS keys.

C.3.5.6.4 Auditor

The contractor shall provide personnel to perform day-to-day auditing of the FPKI, including but not limited to:

- Reviewing, maintaining, and archiving audit logs.
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and Certificate Status Server (CSS) (where applicable) are operating in accordance with its CPS.

The Auditor shall be a separate individual from all other key roles.

C.3.5.7 Documentation Management

The Contractor shall develop, implement and execute a Documentation Management Plan (DMP) that addresses any/all Contractor-generated documentation to include manuals, Standard Operating Procedures (SOPs), Release Notes, Design Documents, Inventory Lists, Functional Specifications, Detailed Requirements, Installation Guides, User Guides, Miscellaneous Procedures, Reports, Whitepapers, and Security Documentation.

All project-related documentation shall be a project deliverable. The contractor shall ensure that the government and all approved contractor personnel are provided the latest approved versions of documentation. The contractor shall deliver the Documentation Management Plan to the GSA and obtain FPKIMA approval. The Document Management Plan shall be managed as part of the overall PMP.

All Contractor provided documentation shall be compatible with Microsoft Office products such as Word, PowerPoint, Excel, Visio, or Access. Due dates for all documents are included in Deliverables outlined in Section F.2. All documents and plans required as deliverables shall be submitted to the GSA within the time-frames specified throughout Section F.2.

The GSA will review the documents for accuracy and completeness, and return them to the contractor with comments as appropriate. The contractor shall make revisions to the documents to address the concerns of the Agency, and re-submit for formal Agency approval. The contractor shall not implement any plans that have not been formally approved by the GSA.

The contractor shall store all delivered documentation on GSA-provided document management systems (e.g. Sharepoint or Google Drive) as directed by the FPKIMA.

C.3.5.8 Inventory Management

The contractor shall develop, implement, and execute an Inventory Management Plan (IMP) that documents all hardware and software components in the FPKI system, regardless of whether they are provided by the contractor or the government. The contractor shall ensure that the Government and all approved Contractor personnel are provided the latest approved versions of the IMP. The Inventory Management plan shall be delivered and managed as a part of the overall PMP.

C.3.5.9 Change and Configuration Management

As a component of the contractor's sustaining engineering support, the contractor shall develop, implement, sustain and follow a rigorous Configuration Management Plan for all systems and subsystems. The purpose of this plan is to maintain the configuration integrity and fidelity of FPKI systems and to affect an orderly, systematic, and traceable evolution of changes necessary in response to changing mission needs or operational requirements.

The contractor shall comply with the GSA Change and Configuration Management Process and NIST SP800-128 for FPKI operations. The contractor shall ensure that the GSA PM is part of the required approvers and shall get their approval for all change requests that would need to go through the Change and Configuration Management process. This process and its associated procedures shall comply with GSA IT Security Configuration and Change Management policies and procedures, and also incorporate industry-standard Project Management Methodology, Systems Engineering Lifecycle Processes and Methodology and applicable portions of Security Systems Engineering as defined by NIST SP 800-160.

The contractor shall maintain a library of accurate and up-to-date configuration management and technical data on GSA-provided document storage systems, to include such items as documentation updates, as-built drawings, and drawing updates with field and design changes.

The contractor shall deliver a completed configuration management plan no later than 1 month following contract award for review and approval by the GSA. Following the initial delivery of the plan, the plan shall be updated and re-submitted to the GSA for revision and approval as a part of the overall PMP. The contractor shall comply at all times with its own Change and Configuration Management Process, as identified in its technical proposal and the Change Management Plan it utilizes on the task order.

C.3.5.10 Equipment Warranty and Software License Management

The contractor shall provide equipment warranty and software license management services to the GSA FPKIMA. Within 90 days of award, the contractor shall assess all hardware and software products utilized within the FPKI infrastructure, and provide a renewal schedule to the FPKIMA. As needed throughout the task order, the contractor shall assist the FPKIMA with managing and coordinating renewals with vendors.

C.3.5.11 Obsolescence Management

The contractor shall provide obsolescence management services to the GSA FPKIMA. Within 120 days of award, the Contractor shall assess all hardware and software products utilized within the FPKI infrastructure, and provide a list of products and the Original Equipment Manufacturer (OEM) obsolescence schedule to the FPKIMA. The contractor shall develop a Product Replacement Plan that assesses options for equipment replacement. The contractor shall discuss and coordinate replacement activities with the FPKIMA. The contractor shall manage and perform all infrastructure updates.

The contractor shall perform obsolescence management activities on an annual basis.

C.3.5.12 Chronic Problem Management

The federal government FPKI infrastructure requires an operational system that provides a consistently high level of performance with people, processes, infrastructure and tools. The contractor shall plan for and address chronic events that repeatedly appear and then disappear, potentially even if contractor personnel have previously taken actions to remediate. The Program Manager shall report chronic problems to the FPKIMA, identify root causes, and provide a plan to mitigate.

The contractor shall establish and utilize processes and tools to allow contractor staff to identify, troubleshoot and correct chronic problems in contractor's network, processes or personnel. The Contractor shall identify problems reported through a variety of paths, including user problem reports, FPKI system network monitoring systems or FPKIMA inputs.

The contractor shall implement processes that specifically identify and track resolution of chronic problems. Problem reports / trouble tickets shall document whether issues are 're-occurring or existing', in addition to 'new'.

For operational problems in the FPKI infrastructure, the contractor's network management system shall provide the GSA with appropriate data analytics to address reoccurrence of the same problem, or a series of related problems that cause, or potentially could cause, performance degradation. Otherwise, the contractor shall perform relevant and thorough analysis. All chronic problems shall be discussed with the FPKIMA to determine the best course of action to correct. Chronic problems that are identified to be personnel-related may result in personnel removal at FPKIMA direction.

C.3.6 Ancillary Support (ref. Alliant C.3.4)

C.3.6.1 Future Technology Analysis and Support Services

The contractor shall assist the GSA PM in adapting to technology changes affecting the FPKIMA and its customer base as follows: (i) conducting strategic planning for all operational, tactical and policy aspects of the FPKI, as requested; (ii) performing studies and analysis related to complex technical issues of the FPKI community, as requested; (iii) and conduct planning and analysis on key areas where the FPKIMA can provide additional value to the FPKI community, as requested.

The contractor shall perform technology research, analysis, design, planning and management. Such tasks include, but are not limited to the following:

- Studies or white-papers that require one-time piece of research designed for a particular purpose, as requested
- Analyses to determine the desired end and the most efficient methods for obtaining specific services, as requested

- Systematic approach to troubleshooting faults within the FPKIMA components and recommending a solution
- Studies, designs, implementation and support of FPKI certificates and processes for machine-to-machine Non-Person Entities (NPE) systems as defined by NIST SP 800-183 that utilize FPKI.
- Improved Continuous Diagnostics and Monitoring processes and tools to incorporate DHS policies, NIST SP 800-184, SP 800-137, and other guidelines as directed by the FPKIMA.
- Implementation of the Federal Risk and Authorization Management Program (FedRAMP) Cloud-Based Certificate Repository Service
- Implementation of any additional FPKI processing sites
- Deployment of approved changes or fixes to the FPKIMA
- Improvement of internal tools (e.g. technical infrastructure, program management, information assurance), and implementation of changes as directed by the FPKIMA
- Any other, currently undefined, system functional updates

C.3.6.2 FedRAMP Cloud-Based Hybrid Content Delivery Network

The Contractor implements a cloud-based Hybrid Content Delivery Network. As directed by the GSA PM, the Contractor shall design a cloud-based Hybrid Content Delivery Network (H-CDN) to support distribution of Federal PKI certificates and the ensuing certificate validation checks.

1. The H-CDN shall utilize highly available services using FedRAMP approved system(s)
2. The H-CDN shall be accessible by the Federal Government using dynamic DNS (e.g. http.fpki.gov) and two (2) static IP addresses with change management. The H-CDN shall support IPv4 and IPv6. Any additional, specific, interface requirements shall be implemented by the Contractor at the request of the FPKIMA during design, integration and testing of the H-CDN.
3. The Contractor-provided certificate distribution capability shall provide highly available (24/7) and reliable repository services, accessible via Lightweight Directory Access Protocol (LDAP) and Hypertext Transfer Protocol (HTTP), and support applications during certificate path discovery and validation.
4. The certificate distribution capability shall enable the transactions of cross-certificates in support of the FPKI.
5. The H-CDN shall be implemented with a redundant, geographically dispersed CONUS service.
6. The H-CDN shall be fully designed, engineered, implemented, tested and deployed within 180 days after the FPKIMA provides direction to initiate the service. The Contractor will complete the IA documentation and approval process and obtain an ATO within that 180 day period.
7. The contractor shall develop an H-CDN Transition-In Plan for how they will extend current certificate distribution capabilities and services using the internal system repository to utilize an external FedRAMP-approved service provider. The contractor shall ensure the FedRAMP services interface and work with the contractor's secure CA operations and associated infrastructure and services. This Transition-In Plan shall be delivered to GSA within 20 business days after the FPKIMA provides authorization to

proceed. The Contractor shall not proceed with implementation until the Contractor has obtained FPKIMA approval.

As part of the H-CDN Transition-In Plan, the contractor shall develop and deliver a contingency plan to enable, if required by the government and approved by the PM and COR, the replacement of the selected FedRAMP certificate distribution service provider with a new FedRAMP service provider. The new FedRAMP service provider shall provide services that meet or exceed the requirements stated in this section.

8. After the cloud-based H-CDN service has been implemented and integrated with the current FPKI infrastructure, this service shall transition to GFE infrastructure.
9. The contractor shall provide Services that enable certificates to be issued by and to the FPKI Trust Infrastructure CAs. The contractor shall support access to these certificates via the repository for external partner applications. This certificate distribution capability shall connect to, and extend, the operations of the existing repository. Interoperation with cross-connected Federal CA's shall transfer to the certificate distribution capability.
10. The contractor shall provide Services such that external partners can utilize the CRLs in the FPKI Repository to validate and check status of cross-certifications between the FPKI and external partners. The contractor shall provide services such that FPKI CA CRLs shall be published in the FPKI Repository twice daily, at a minimum.
11. The contractor shall provide products, services, and capabilities to support the provision of publicly accessible repositories and services (i.e., PKI directories and certificate status responders) that provide certificate status information to requesting applications and services.
12. The contractor H-CDN capability shall provide services such that it is able to ensure the availability of operations to provide required services at a 99.96 percent uptime or better level. The contractor shall ensure services are provided at an infrastructure that is highly available (24/7) and has fault-tolerant hardware/software redundancy, redundant facilities, load balancing, fail-over capability, and automated and manual system monitoring and administration to ensure to meet the required uptime/operations level.
13. The contractor shall provide services with capabilities to support a minimum growth rate of repository and transactions of 20% per year for each year of the task order. However, due to the anticipated growth in NPE devices, the Contractor shall anticipate and design for significantly higher traffic growth.
14. The H-CDN shall be designed to evolve over time to withstand changing rapidly changing cyber-attacks, including Distributed Denial of Service (DDoS) attacks, malware delivery, domain name changes, etc.
15. The Contractor shall implement a continuous monitoring performance dashboard as part of the H-CDN capability.
16. The H-CDN shall be operable 24 hours per day, 7 days per week, including all Federal holidays.
17. The FedRAMP certificate distribution capability supporting the FPKI shall be able to meet the requirements to achieve a FISMA Authorization to Operate (ATO) at the FIPS 199 GSA lightweight SaaS level.

C.3.7 Information Assurance and Cyber Protection

The FPKI Solution will reside outside of Agency networks and beyond the Trusted Internet Connection (TIC) boundaries unless future direction is provided by the FPKIMA. The System shall comply with GSA information security policy. Cyber protection services provided by the Contractor shall include protecting all services, information, infrastructure, and information processing resources against threats, attacks, or failures of systems.

To secure access to any system applications, the FPKI Infrastructure Solution shall support user identification and authorization through the use of PIV cards, unless the FPKIMA grants an exception for using other login methods. The user credential information shall be protected and shall not be transmitted in the clear between user and application systems.

Pursuant to the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002, P.L. 107-347, the contractor shall implement minimum security controls required to protect Federal information and information systems to the level identified by the Government. The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

The contractor shall provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; or information systems used or operated by an agency or by a contractor of an agency. This applies to individuals and organizations having contractual arrangements with the GSA, including employees, contractors, vendors, and outsourcing providers, which use or operate information technology systems containing GSA data.

The FPKI contractor shall meet the requirements of Moderate security impact level in accordance with FIPS 199, 200, other relevant NIST Special Publications (SP) for the FPKI pre-production, production, and disaster recovery services, excluding the laboratory system. The FPKI contractor shall also meet the requirements of any GSA-modified controls.

The contractor shall plan for a potential transition to a FIPS 199 high security impact level for the production of operational FPKIMA facilities, including the pre-production, primary and disaster recovery facilities but excluding the laboratory. This transition plan shall also include any architectural components added during contract execution, such as the optional FedRAMP Cloud-Based Hybrid Content Delivery Network Service.

Any transition to a FIPS 199 high security impact shall require a comprehensive vendor plan addressing the recommended technical approach, implementation options, risks, staffing and costs at a minimum. The contractor-provided plan shall require Government evaluation, Contractor modifications, and Government approval with all relevant stakeholders.

The contractor's facilities supporting the FPKI shall be able to meet the requirements to achieve a FISMA Authorization to Operate (ATO) at a FIPS 199 high security impact level / DoD Top Secret level.

The contractor shall ensure that all applicable products used in operations, maintenance, or delivery of this task order is Common Criteria certified or evaluated and approved by GSA.

The FPKI system (GFE-provided and Contractor-provided infrastructure) is considered a High Value Asset as identified by the GSA per OMB M-17-09, and shall be subject to all relevant oversight processes, including documentation reviews, site and document audits which may be announced or unannounced. At the discretion of GSA FPKIMA Cyber security, a FISMA Contractor review shall be conducted by the Government, and the Contractor shall provide all necessary support.

All portions of the solution shall fully comply with security requirements which may change during the contract period. The Contractor shall propose a mitigation strategy if the solution security cannot adhere to any imposed security requirements.

The solution security features and performance will be audited regularly by the GSA, and the Contractor shall address any identified susceptibility in any security aspect of the system promptly.

The contractor shall report and remediate all disclosed and identified security risks and flaws per IAW GSA IT Policy. All flaws must be tracked within the Plan of Actions and Milestones (POA&M).

C.3.7.1 Contractor Personnel

The contractor and its subcontractors shall only utilize U.S. citizens with Top Secret clearances for all personnel performing work or supporting this task order. The contractor shall assure that all its technical and operational personnel, including all subcontractor personnel, shall be qualified to become HSPD-12 credential holders.

The contractor shall remove any personnel from the program immediately as directed by the FPKIMA.

The contractor shall not remove or change any of the Key Personnel without providing at least 30 days written notice to the GSA which documents the rationale for the change. In the case any key personnel are removed from the program, the contractor shall notify the CO, COR and FPKIMA within 24 hours of being aware of any removal decision.

The contractor shall identify suitable replacements for key personnel within 10 business days of any notice for personnel removal. The contractor shall provide resume(s) to the FPKIMA who shall retain the right to accept or reject any proposed candidate(s).

Additional requirements pertinent to key personnel and FPKI/Trusted Operations personnel are listed in L and C.3.5.6.

C.3.7.2 Data Handling and Markings

Data shall be subject to privacy protection in accordance with the Privacy Act of 1974, as amended. The contractor shall mark and control data as directed by the FPKIMA throughout task order execution to comply with evolving GSA policies and directives.

If the deliverable or document is considered to be classified, the preparation of the document shall in addition be conducted at a cleared government facility.

C.3.7.3 Safeguarding / Protecting Sensitive Personally Identifiable Information (PII)

All FPKI data shall be protected by the Contractor per all relevant Federal and GSA mandates associated with PII data including 2180.1 CIO P GSA Rules of Behavior for Handling Personally Identifiable Information (PII). The Contractor shall comply with 9297.B, CIO GSA Information Breach Notification Policy for the protection and reporting of any data breaches. The contractor must ensure that personnel data, specifically PII, processed or stored within the FPKI System is properly reported to the GSA Privacy Officer and, if necessary, support development and maintenance of the System of Record Notification (SORN).

C.3.7.4 Handling Information Security Incidents

The GSA CIO defines incidents as "a violation or imminent threat of violation of information security or privacy policies, acceptable use policies or standard security practices." The contractor shall maintain procedures for detecting, reporting, and responding to security incidents, and mitigating risks associated with such incidents before substantial damage is done to federal information or information systems. The contractor shall immediately report all computer security incidents that involve GSA information systems to the GSA IT Service Desk (ITServiceDesk@gsa.gov or 1-866-450-5250). Any theft or loss of IT equipment with federal information / data must be reported within one hour of the incident to the GSA. Incidents involving the loss or theft of sensitive but unclassified (SBU) data shall be reported to GSA Service Desk and the FPKIMA.

The contractor shall report (potential or confirmed) incidents for lost or stolen GSA-owned devices, which includes mobile phones, tablets, laptops, token keys, USB drives or GFE FPKI infrastructure systems. The contractor shall also report unauthorized access to PII or other sensitive data, plus any malicious code, improper use, or scans/probes/attempted access that are detected.

C.3.7.5 Defense Information Systems Agency (DISA) Application Security

The contractor shall implement Application Security and Development guidelines established by the Defense Information Systems Agency (DISA) as directed by the GSA.

C.3.8 Transition-In Requirements

The contractor shall provide transition-in services for the FPKI services and operational infrastructure. The contractor shall develop and execute a transition-in plan that encompasses at a minimum:

- Providing qualified personnel to provide all FPKI services
- Knowledge transfer from the incumbent contractor, to include:
  - Contractor personnel notes
  - Personnel shadowing
  - any in-process documentation not yet delivered to the GSA,
  - Standard Operating Procedures
  - All official project documentation
  - Inventory Lists
- Assuming leadership and ownership of all activities collaboratively with the incumbent Contractor.
- Audit of published documentation to validate current system descriptions, operational procedures, etc. accurately reflect the current system.
- Deployment of data center infrastructure and any equipment and connectivity moves
- Account Management
- Transfer of any hardware warranty or software license contracts held by the incumbent support contractor.

The contractor shall provide all necessary infrastructure items with the exception of the GFE infrastructure. Assumption of operational roles shall be completed within 90 days of task order award.

As requested by the contractor, the government will extend leases with the incumbent Provider for any infrastructure leases (e.g. data centers, telecommunications circuits, misc. infrastructure items) for a period not to exceed 3 months.

C.3.9 Transition-Out Requirements

The contractor shall provide clear, collaborative, and effective transition-out support of all activities, knowledge, and infrastructure to any follow-on provider. The Contractor shall submit a transition-out plan to the GSA within 120 days after task order award for FPKMI review and approval.

The contractor's transition-out plan shall include extending leases for any contractor-provided infrastructure for a period not to exceed 180 days after award of any follow-on contractor to another provider. The contractor's transition-out plan shall also address return of any GSA-provided items such as laptops and phones within 15 days in an orderly manner, handover of all documentation, change-over of PKI and any system password access, to best provide FPKI continuity of service during the transition to the follow-on contractor.

C.3.10 Relevant Documents

Cyber and FPKI certificate policies for the Federal Government are continually evolving. The contractor shall provide a FPKI infrastructure support service that is compliant with policies outlined below, as well as any future updates, additional pertinent documents not listed, or emerging policies not yet issued.

Table C-1: Applicable Documents – Office of Management and Budget

Office of Management and Budget (OMB)	
A-130	Managing Information as a Strategic Resource, 27 July 2016
A-123	Management's Responsibility for Enterprise Risk Management and Internal Control, 15 July 2016
M-17-09	Management of Federal High Value Assets, 9 December 2016
M-17-05	Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements
M-16-04	Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, 30 October 2015
M-15-13	Policy to Require Secure Connections across Federal Websites and Web Services, 8 June 2015
M-14-03	Enhancing the Security of Federal Information and Information Systems
M-11-11	Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
M-09-32	Update on the Trusted Internet Connections Initiative, 17 September 2009
M-08-27	Guidance for Trusted Internet Connection (TIC) Compliance, 30 September 2008
M-07-16	Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 22 May 2007
M-06-18	Acquisition of Products and Services for Implementation of HSPD-12, 30 June 2006
M-05-04	Policies for Federal Agency Public Websites, 17 December 2004
M-04-04	E-Authentication Guidance for Federal Agencies, 16 December 2003

Table C-2: Applicable Documents – Department of Homeland Security

Department of Homeland Security (DHS)	
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors
HSPD-12	System Infrastructure Provider to FPKI Shared Service Provider Interface Specification, 7 February 2007

Table C-3: Applicable Documents – National Institute of Standards and Technology

National Institute of Standards and Technology (NIST)	
800-53	Security and Privacy Controls for Federal Information Systems and Organizations, April 2014
800-53A Rev4	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, December 2014
SP 800-60 Vol II Rev 1	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-63-2	Electronic Authentication Guideline, August 2013
800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Sept 2011
SP 800-39	Managing Information Security Risk Organization, Mission, and Information System View, March 2011
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle, April 2014
FIPS PUB 140	Security Requirements for Cryptographic Modules
FIPS PUB 180	Secure Hash Standard
SP 800-57	Recommendation for Key Management
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-102	Recommendation for Digital Signature Timeliness

SP 800-131A	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
SP 800-160	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016
SP 800-184	Guide for Cybersecurity Event Recovery
SP 800-183	Networks of 'Things', July 2016
SP 800-128	Guide for Security-Focused Configuration Management of Information Systems, August 2011
SP 800-125	Guide to Security for Full Virtualization Technologies, January 2011
SP 800-123	Guide to General Server Security, July 2008
SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
SP 800-119	Guidelines for the Secure Deployment of IPv6, December 2010
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems

Table C-4: Applicable Documents – Federal PKI Policy Authority

Federal PKI Policy Authority (FPKIPA)
Federal Public Key Infrastructure (FPKI) Compliance Audit Requirements, Version v2.0.1, 10 July 2015
Non-Compliance Management Framework for the Federal Public Key Infrastructure (FPKI), Version 1.0.1, 6 January 2016

Table C-5: Applicable Documents - Presidential Directives

Presidential Directives	
	Cybersecurity National Action Plan (CNAP)
EO 13693	Executive Order 13693, Planning for Federal Sustainability in the Next Decade, 25 March 2015

Table C-6: Applicable Documents - Industry Standards

Industry Standards	
ANS ANS X9.80	Prime Number Generation, Primality Testing and Primality Certificates
PKCS #1	Public Key Cryptography Standard, RSA Encryption Standard

C.3.11 Service Level Agreements (SLA)

The FPKI infrastructure, support and services provided by the Contractor shall be provided within performance requirements as outlined below.

Table C-7: Service Level Agreements – FPKI Transaction / Process

FPKI Transaction / Process	Minimum Performance Standard
Availability of the CAs, certificate status information services and operations	99.9% measured on a monthly basis (no more than 44 minutes/month unscheduled downtime)
Certificate Generation and Delivery	In accordance with the applicable Certificate policies
Test and publish the completed cross-certificates it issues	In accordance with the applicable Certificate policies
Provide Certificate Lifecycle Management, including: ● Certificate issuance ● Certificate content maintenance ● Certificate renewal ● Certificate revocation and suspension upon an authenticated request ● Certificate authority key rollovers	In accordance with the applicable Certificate policies
Provide for the publication of Certificate status information	In accordance with the applicable Certificate policies
Provide for OCSP Response (if implemented)	In accordance with the applicable Certificate policies

Table C-8: Service Level Agreements – Support Service

Support Service	Minimum Performance Standard

Standard / Routine Trouble ticket tracking and management services	Available 5 days per week, Monday through Friday except Federal Holidays, between hours of 9am to 5pm US eastern time.
On-call operational staff response to automated notification of system or system component outages	● Available 24 hours, 7 days per week, including Federal Holidays. ● Contractor staff shall comply with staffing requirements for trusted roles as documented in the CP/CPS documents. ● For failures of redundant components where the system remains operational, staff shall arrive onsite within 24 hours to triage.
Complete transition-in (assumption of operational role for the FPKI system)	Within 90 days of task order award
Move the backup site to contractor-proposed location	Within 90 days of task order award
Move the primary site to contractor-proposed location (if shift is proposed)	Within 180 days of task order award; the primary site move shall not overlap with the backup site move.
Operation of FPKI system in a non-redundant state during any infrastructure moves	Move to be completed within 24 hours of initiating shutdown / cable disconnects of the site that is moving
Obtain and maintain Authority to Operate (ATO) for the production systems (both sites), pre-production and laboratory sites	Obtain within one year after task order award. Maintain throughout life of task order.
Implementation of any similar production, pre-production or laboratory sites	Within 180 days of completion of GSA/Contractor planning activities and official FPKIMA notification to proceed.
Implementation of optional FedRAMP cloud-based Hybrid Content Delivery Network	Within 180 days of completion of GSA/Contractor planning activities and official FPKIMA notification to proceed
Update of the ATO to document systemic architecture changes (e.g. new FPKI processing site(s), FedRAMP cloud-based Hybrid Content Delivery Network)	Within 180 days of completion of GSA/Contractor planning activities and official FPKIMA notification to proceed